Packet Dropping Attack in MANET

Rakesh Kumar ER
Asst. Prof & Head,
Computer Science and Engineering,
SAMS College of Engineering and Technology, Chennai

***Abstract* - Mobile Ad-hoc NETwork (MANET) is an application of wireless network with self-configuring mobile nodes. MANET does not require any fixed infrastructure. Its development never has any threshold range. Nodes in MANET can communicate with each other if and only if all the nodes are in the same range. This wide distribution of nodes makes MANET vulnerable to various attacks, packet dropping attack or black hole attack is one of the possible attack. It is very hard to detect and prevent. To prevent from packet dropping attack, detection of misbehavior links and selfish nodes plays a vital role in MANETs. In this paper, a comprehensive investigation on detection of misbehavior links and malicious nodes is carried out.**

***Keywords* - MANET; Packet dropping attack; Black hole attack**

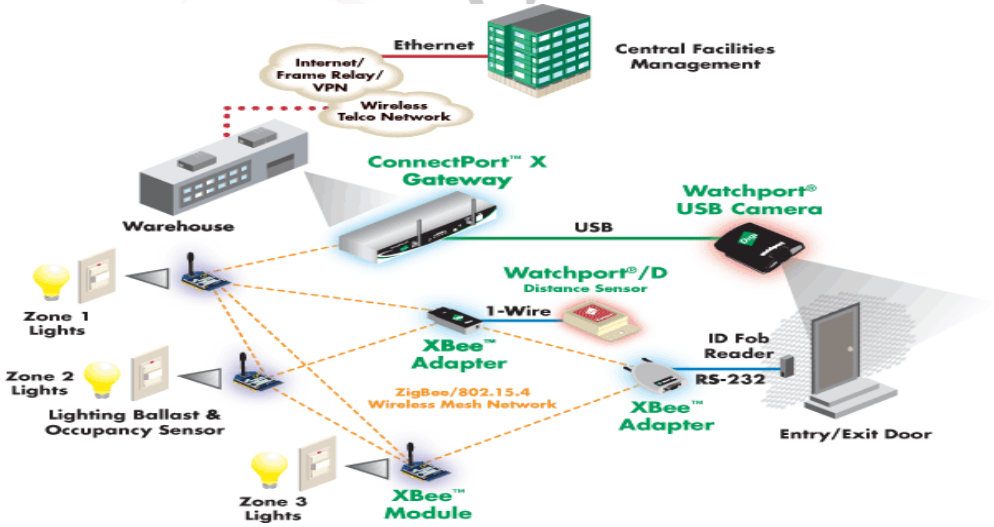
I. INTRODUCTION

Mobile Ad-hoc NETwork (MANET) is a self-configuring network consisting of nodes working cooperatively in ad-hoc manner without a fixed network infrastructure [9], [22]. Each node in a MANET is mobile and is free to move in a random fashion. The salient distinct feature of MANET is the dual behavior of each node, where it acts as both router and host. MANET nodes include cell phones, laptops etc., have limited computation, communication and energy resources. MANET is much more vulnerable to attacks [1], [2], [5], [13], [25] as compared to a wired network due to the following factors:

- Complex security solutions cannot be used because nodes have limited energy.
- Packet transmission is done in wireless medium.
- There is no central management point, which makes it difficult to ensure that all nodes participating in the network are benign.
- Mobility of nodes makes routing even more challenging as the topology keeps changing regularly.

Having mentioned the general issues in MANETs, the reason behind their popularity and their benefits are,

- Low cost of deployment: Ad-hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.
- Fast deployment: Ad-hoc networks are very convenient and easy to deploy when compared to WirelessLANs (WLAN), since it requires less manual intervention.
- Dynamic Configuration: Ad-hoc network configuration can change dynamically with time. It is very easy to change the network topology when compared to configurability of LANs.



Attacks can be launched from all layers of the protocol stack [2], [5], [23] but the routing layer attacks are the most damaging. Malicious code and repudiation are done in application layer. Session hijacking and flooding are done in transport layer. Sybil, flooding, black hole, grey hole, worm hole, link spoofing, link withholding, location disclosure etc., are done in network layer.

Malicious behavior, selfish behavior etc., are done in data link/MAC layer. Interference, traffic jamming, eavesdropping etc., are done in physical layer.

A routing protocol [13], [24] specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge about the networks attached to it directly. A routing protocol shares this information among immediate neighbors, and then throughout the network. The routing protocol is classified into proactive and reactive protocols.

Proactive protocols are table driven, all routing decisions are made by the nodes based on their predetermined routes. Every participating node maintains routing information in a routing table. In proactive routing, route discovery is easy and route maintenance is hard due to the dynamic topology of the network. Destination Sequenced Distance Vector (DSDV) and Fisheye State Routing (FSR) protocol are some of the most popularly used table-driven protocols. Proactive protocols find the least cost to reach the destination.

Reactive protocols are on-demand [7], [8], the routes are discovered when a node desires to send a packet. Two main processes involved are route discovery and route maintenance. Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance Vector (AODV) are some of the most popularly used on-demand driven protocols. Reactive protocols find the minimum hop count to reach the destination. Both of these protocols fail to consider other important QoS parameters like bandwidth, jitter, node energy level, queue length etc. In the next section, a survey of the state-of-the-art of Packet dropping attack on the network layer is discussed.

II. PACKET DROPPING ATTACK

In MANET, a packet dropping attack is a type of denial of service in which a node in the network will drop the packets instead of forwarding them, which is shown in the fig 1. The packet dropping attack [3], [6], [11] is very hard to detect and prevent because it occurs when the node becomes compromised due to a number of different causes. The packet dropping attack in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack.

- The malicious node can intentionally drop all the forwarded packets going through it (black hole).
- It can selectively drop the packets originated from or destined to certain nodes that it dislikes.
- A special case of black hole attack dubbed gray hole attack is introduced. In this attack, the malicious node retains a portion of packets (one packet out of N received packets or one packet in a certain time window), while the rest is normally relayed.

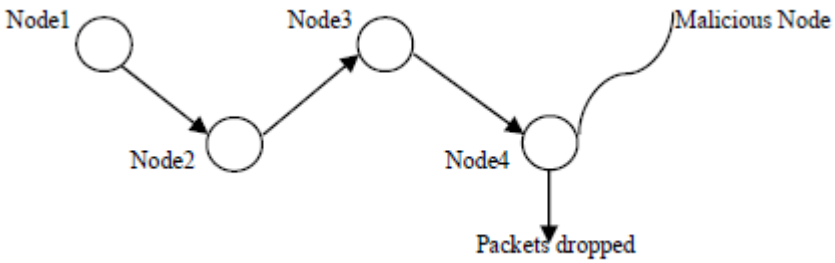


Fig 1: Packet Dropping Attack

The compromised node will broadcast the message [11], [12] that it has the shortest path towards a destination to initiate packet dropping attack. Hence, all packet transmissions will be directed through the compromised node, and the node is able to drop the packets. If the malicious node attempts to drop all the packets, the attack can be identified through common networking tools. Moreover, when other routers notice that the compromised router is dropping all packets, they will generally begin to remove that router from their

forwarding table. Hence, there is no packet transmission through the compromised node. However, it is often harder to detect the packet dropping attack, if the malicious router begins dropping packets on a specific time period or over every n packet, because some packet transmission still flows across the network. For the prevention of packet dropping attack, detection of selfish nodes [6], [11], [12], [17] plays a vital role in MANETs.

III. SELFISH NODES DETECTION IN MANET

Recently, several approaches were proposed to deal with malicious attacks. In this section some of the existing approaches which are mainly used for detecting and mitigating routing misbehavior are discussed.

Watchdog approach

Marti [16] used watchdog and path rater approaches for detecting and extenuating routing misbehavior as shown in figure 2. Source node S can send the data packets to the Destination node D, if there exists a direct connection between S and D. Otherwise, the source node should rely on intermediate nodes. Hence, before forwarding the packets, the misbehaving nodes should be detected.

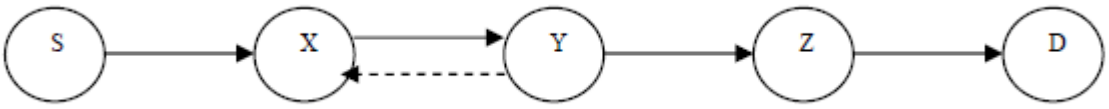


Fig 2: Watchdog Approach

In fig 2, there is a path from S to D through the intermediate nodes X, Y and Z. The solid line represents the intended direction of the packets sent by S to D. The dashed line indicates that X is within the transmission range of Y and overhears the packet transfer. The source node S sends the packet to X which in turn forwards to Y. When Y forwards a packet to Z, X overhears Y's transmission and verifies that Y has forwarded the packets to Z.

Many MANET IDSs are developed [14], [18] as an improvement to the watchdog approach. Watchdog approach fails to detect a misbehaving node in the presence of,

- Ambiguous collisions - It prevents X from overhearing Y's transmission if other neighbors send packets to X at the same time.
- Receiver collisions - In this problem, node X checks whether Y sends the packet to Z, but not the reception at Z.
- Limited transmission power - The intermediate nodes may not send the reports if it has limited transmission power.
- False misbehavior - It occurs when nodes falsely report about other nodes.
- Collusion - If collusion occurs in multiple nodes then it will affect packet transmission.
- Partial dropping – It occurs if a node drops fewer packets.

Path rater

The path rater picks the reliable route based on the knowledge of misbehaving nodes and link reliability data. It is used by each node in the network. Each node maintains a rating for every neighboring nodes. A path metric is calculated by averaging the node ratings in the path. The shortest length path algorithm is used to find the shortest distance path from source to destination based on this metric value.

Collaborative security architecture

Patcha [19] used an extension approach to the watchdog approach. In this approach, the nodes in the network are classified into trusted and ordinary nodes. The nodes which are involved in initial network formation are called as trusted nodes. The nodes which are joining later in to the network are called as ordinary nodes. The ordinary node can be promoted as trusted node if the node proves its trustworthiness. Another assumption in this approach is that all the trusted nodes should not be a malicious or selfish node. The watchdog nodes are selected from the set of trusted nodes for a given period of time based on the node energy, available node storage

capacity and node computing power. The watchdog node has the additional duty to monitor other nodes in the network for a fixed period of time to detect the malicious behavior. Watchdog node maintains two threshold values SUSPECT_THRESHOLD and ACCEPTANCE_THRESHOLD to measure the trustworthiness of the non trusted nodes. If any node crosses the SUSPECT_THRESHOLD, it will be declared as malicious node by the watchdog node. If a node crosses the ACCEPTANCE_THRESHOLD, it will be declared as trusted node. The existing AODV protocol was extended with six extra packet types send_data, nodes_neighbors, trusted_enc_request, trusted_enc_reply, is_watchdog and is_malicious to implement the security. However, theadditional packet types increases the network overhead.

Cross layer approach

Djenouri [4] used a cross-layer approach to detect data packet droppers. In this approach, the two parts of the monitoring protocol are used in network layer and MAC layer. Each node monitors the forwarding of each packet it transmits, like watchdog approach. To reduce the network overhead, for each received packet the node transmits two-hop ACK integrated with MAC ACK. To prevent an intermediate node from falsifying two-hop ACK, public key distribution is used in this approach. To reduce the cost of this approach, random two-hop ACK is used. In this approach, a random ACK is transmitted in every three consecutive nodes instead of transmitting ACK for every data packet. A node will select an even number if it needs an ACK, otherwise it will select an odd number. This approach increases the network overhead due to public key distribution.

Collaborative watchdog approach

Hernandez [6] used a collaborative watchdog approach to reduce the detection time of selfish nodes in the network, based on contact dissemination. In this approach, initially the collaborative node does not have any information about the selfish nodes. The collaborative node gets the information about the selfish node when a contact occurs based on either as a selfish contact or as a collaborative contact. When the watchdog node receives packets from a new node it is considered as a new contact. Then, the node transmits a message specifying all known selfish nodes to this new node. The main overhead of this approach is the number of messages needed for this transmission. Moreover, the effects of false positives and false negatives are not measured.

TWOACK approach

Liu [15] used TWOACK and Selective TWOACK (S-TWOACK) approaches. TWOACK approach detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from source to destination. Each

node in the path is required to send an acknowledgment packet. It is neither an enhancement nor a watchdog based approach. It is required to work on routing protocols such as DSR[10].

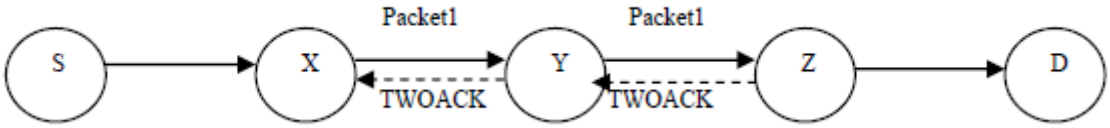


Fig 3: TWOACK Approach

TWOACK approach requires an explicit acknowledgment to be sent by Z to notify X about the successful reception of the data packet. When node Z receives the data packet successfully, it sends a 2ACK packet to X with the id of the corresponding data packet. The TWOACK transmission takes place for every set of triplets along the route, as shown in the fig 3. This approach is mainly used to resolve the receiver collision and limited transmission power problems of watchdog approach. Cost is the main overhead of this approach since it requires a two-hop ack for every data packet. In S-TWOACK scheme, each TWOACK packet acknowledges the receipt of all the data packets over the period of time.

2ACK

Liu [15] used 2ACK approach to mitigate the adverse effects of selfish nodes. It is based on a simple 2-hop acknowledgment packet. The receiver node in the 2ACK scheme sends 2ACK packets only for a fraction of received data packets. It has an authentication mechanism to make sure that the 2ACK packets are genuine. This reduces the network overhead by minimizing the number of ACK packets and also it is cost effective. However, it focuses only on link behavior rather than a single node.

Adaptive ACKnowledgment scheme (AACK)

Sheltami [20] used an Adaptive acknowledgment scheme, a network layer acknowledgment based scheme in which the TwoAck and end-to-end schemes are combined. In this approach, if a sender has more than one destination in the network, it will operate in two different modes, AACK mode and TACK mode. A switching system is used to enable a node to work in two different modes. The default mode of the switching system is AACK mode. The source node will inform to the intermediate node about the flow mode, so that the intermediate node will forward the packets in AACK mode, or it will send TWOACK packet to the previous two hop node in TACK mode.

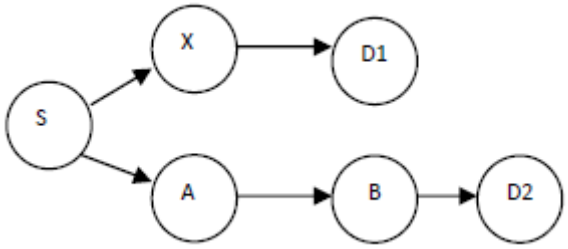


Fig 4: AACK Approach

In the fig 4, a source node S has two flows, S-X-D1 and S-A-B-D2. The switching system will enable the source node to operate in AACK mode for the path S-A-B-D2 since it has more than two hops, and in TACK mode for the path S-X-D1.

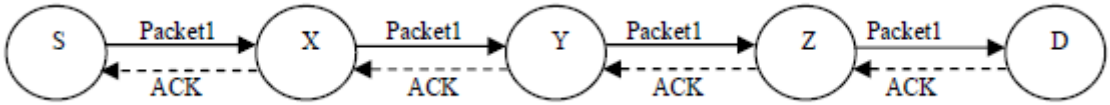


Fig 5: Packet Transmission in AACK Mode

In AACK mode, the destination node sends only one ACK packet to the source node instead of sending ACK packet for every three consecutive nodes. When the destination node D receives the data packet1 from the source node S through intermediate nodes X, Y and Z, it is required to send an ACK packet to the source node, as shown in the fig 5. Hence, it reduces the network overhead. But, both TWOACK and AACK fail to detect the malicious node with the presence of false misbehavior report and forged acknowledgment packets. This scheme is used to overcome collisions and limited transmission power problem of watchdog approach. Moreover it improves the TWOACK scheme. However, in AACK mode, the long path causes packet dropping attack due to significant delay.

Enhanced Adaptive ACKnowledgment scheme (EAACK)

Shakshuki [21] used an acknowledgement based detection scheme Enhanced AACK approach consists of three parts, ACK, Secure ACK (S- ACK), and Misbehavior Report Authentication (MRA). ACK is based on end-to-end acknowledgment scheme. In ACK mode, the source node S will send an ACK data packet to the destination node D through the intermediate nodes. The destination node D will receive the ACK data packet successfully, if all the intermediate nodes are cooperative. After receiving the ACK data packet, the destination node D will send an ACK acknowledgment packet through the same route as shown in the fig 4. If S receives this ACK acknowledgment packet within a predefined time period, then the packet transmission from S to D is successful. Otherwise, node S will switch to S-ACK mode by sending out an SACK data packet.

In S-ACK mode, for every three consecutive nodes in the route the third node is required to send an S-ACK acknowledgment packet to the first node, as shown in the figure 3. The three consecutive nodes work in a group cooperatively to detect misbehaving nodes in the network. It is an improved version of TWOACK scheme. In TWOACK approach, the source node immediately trusts the misbehaving report, whereas in EAACK scheme, the source node will switch to MRA mode to conform the misbehaving report.

In MRA mode, the source node will send MRA packet to the destination node through different paths for authentication, as shown in the fig 6. When the destination node receives the MRA packet through some route then it will compare the MRA packet with its local knowledge base. If the MRA packet is already received through the same route then it will conclude that a node in that route has generated the misbehavior report is marked as malicious. Otherwise, the MRA packet is trusted and accepted.

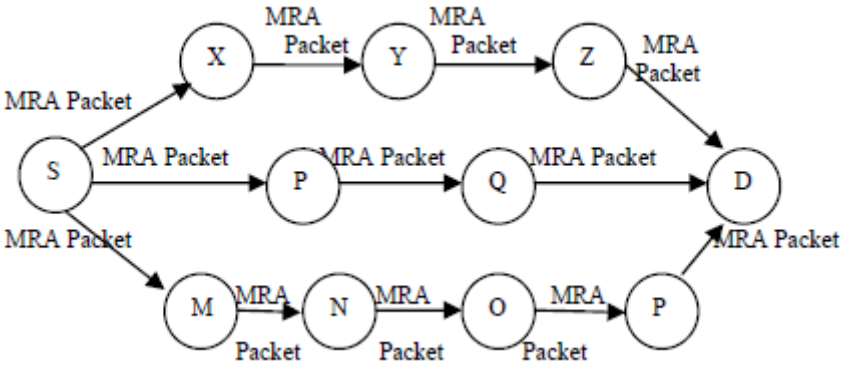


Fig 6: Packet Transmission in MRA Mode

Digital signature is used in this approach. For each communication process, both the source node and the destination node are not malicious. All packets are required to be digitally signed by its sender and verified by its receiver. This approach resolves false misbehavior, limited transmission power and receiver collision problems of watchdog approach. However, it will not detect partial dropping of packets by the intermediate malicious nodes.

IV. Conclusion

Packet-dropping attack has always been a major threat to the security in MANET. In this paper we have presented a survey of the state-of-the-art on securing MANETs against packet dropping attack. Most of the existing approaches are used to detect only the misbehavior links rather than the malicious nodes. Moreover, they fail to detect partial dropping of packets in MANET. The detection of packet droppers in MANETs is a challenge even though many approaches have been proposed against packet dropping attack. Some approaches that rely on cryptography and key management are too expensive. Each approach can work only with specific attack. The approaches that work well in the presence of one malicious node are not suitable for multiple colluding attackers. The focus on all possible types of attack for more secure and reliable MANET with minimizing the cost can still improve the effectiveness and efficiency of the security schemes.

References

[1] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad-hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[2] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad-hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.

[3] S. Djahel, F.N. Abdesselam, Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks : Proposals and Challenges, IEEE Communications Surveys & Tutorials, Vol.13, No.4, Fourth Quarter 2011.

[4] D. Djenouri, N.Badache, Cross-Layer Approach to Detect Data Packet Droppers in Mobile Ad-Hoc Networks, IWSOS 2006, LNCS 4124, pp.-163-176, 2006.

[5] P.Goyal, S.Batra, Ajit Singh, A Literature Review of Security Attack in Mobile Ad-hoc Networks, International Journal of Computer Applications, Vol.9, No.12, November 2010.

[6] E. Hernandez, M.D. Serrat, Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog, IEEE Communications Letters, Vol.16, No.5, May 2012.

[7] Y.Hu, D.Johnson and A.Perrig, " SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3-13.

[8] Y.Hu, A.Perrig, and D.Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in proc. 8th ACM Int.Conf.MobileCom, Atlanda, GA, 2002, pp. 12-23.

[9] G. Jayakumar and G. Gopinath, "*Ad-hoc* mobile wireless networks routing protocol—A review," *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582,2007.

[10] D.Johnson and D.Maltz, "Dynamic Source Routing in ad hoc wireless networks," in mobile computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153-181.

[11] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
[13] B.Kannhavong, H. Nakayama, Y.Nemoto, Nei Kato, A Survey of Routing Attacks in Mobile Ad-Hoc Networks, IEEE Wireless Communication,1536-1284/07, October 2007.
[14] J.S.Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans.Ind.Electron., vol. 55, no. 4, pp. 1835 – 1841, Apr. 2008.
[15] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, An Ac-knowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs. In the IEEE Transactions on Mobile Computing, vol. 6, pp. 536-550, 2007.
[16] S. Marti, T.J. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehaviour in Mobile Ad-hoc Networks. In the Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM, pp. 255-265, Boston, Massachusetts, US, 2000.
[17] N.Nasser and Y.Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24-28, 2007, pp. 1154-1159.
[18] J.Parker, J.Undercoffer, J.Pinkston, and A.Joshi, "On intrusion detection and response for mobile ad hoc networks," in proc. IEEE Int.Conf.Perform.,Comput.,Commun., 2004, pp. 747 – 752.
[19] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad-hoc networks," in *Proc. Radio Wireless Conf.*, 2003, pp. 75–78.
[20] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, A. Mahmoud, "Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs", International Journal of Multimedia Systems, Springer, vol. 15, issue 5, pp. 273-282, 2009.
[21] E. Shakshuki, N. Kang, T. Sheltami, EAACK – A Secure Intrusion – Detection System for MANETs. In IEEE Transactions on Industrial Electronics, Vol.60,No.3,March 2013.
[22] B.Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.
[23] B. Wu, J. Chen, J. Wu, M. Cardei, A Survey of Attacks and Countermeasures in Mobile Ad-hoc Networks, Wireless/Mobile Network Security, Springer, Vol.17, 2006.
[24] M.Zapata and N.Asokan, "Security ad hoc routing protocols," in proc. ACM workshop wireless security., 2002, pp. 1-10.
[25] L.Zhou and Z.Haas, "Securing ad-hoc networks," IEEE networks,vol. 13,no. 6,pp. 24-30, Nov./Dec. 1999.